

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-200125

(43)Date of publication of application : 21.07.1992

(51)Int.Cl.

H04K 1/04
H04N 7/167

(21)Application number : 02-333950

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 29.11.1990

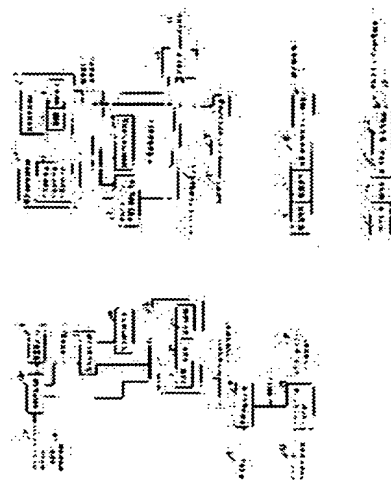
(72)Inventor : INOUE TETSUYA
HARADA YASUO
NEZU SHUNICHI

(54) METHOD AND DEVICE FOR SCRAMBLE CONTROL

(57)Abstract:

PURPOSE: To improve the convenience of use by providing a means deleting forcibly key information in a receiver with a control signal from a transmission station to the device so that descrambling of the receiver once enabling descrambling of a transmission signal is disabled.

CONSTITUTION: When it is required to cancel the permission by a transmitter to a receiver which receives descramble enable information 10 including a destination code 9, key information 6, a key identifier 7, and a key valid period 8, a key control information generating means 14 receiving a device identifier 1 and a key identifier 7 generates key control information 16 including the destination code 9 being the device identifier 1 and information 15 representing invalid key information indicated by the key identifier 7 and sends the information 16 to a receiver via a multiplexer means 4. The receiver uses a destination collation means 20 to input the information 16 to a key collation means 25 when the destination code 9 in the key control information 16 is its own device identifier 1. The collation means 25 uses a key information delete means 26 to delete the relevant key identifier 7 and the key information 6 in pairs from a key storage buffer 21 when the same key identifier as the key identifier 7 sent in the key control information 16 is in existence in the key storage buffer 21.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

BEST AVAILABLE COPY

[Date of requesting appeal against examiner's decision
of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

NOT AVAILABLE COPY

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A) 平4-200125

⑮ Int. Cl.⁹

H 04 K 1/04
H 04 N 7/167

識別記号

庁内整理番号

7117-5K
8324-5C

⑬ 公開 平成4年(1992)7月21日

審査請求 未請求 請求項の数 3 (全6頁)

⑭ 発明の名称 スクランプル制御方法及びその装置

⑯ 特 願 平2-333950

⑰ 出 願 平2(1990)11月29日

⑱ 発 明 者	井 上 哲 也	大阪府門真市大字門真1006番地	松下電器産業株式会社内
⑱ 発 明 者	原 田 泰 男	大阪府門真市大字門真1006番地	松下電器産業株式会社内
⑱ 発 明 者	根 津 俊 一	大阪府門真市大字門真1006番地	松下電器産業株式会社内
⑲ 出 願 人	松下電器産業株式会社	大阪府門真市大字門真1006番地	
⑳ 代 理 人	弁理士 小 鍛 治 明	外 2 名	

明 細 書

1. 発明の名称

スクランブル制御方法及びその装置

2. 特許請求の範囲

(1) 伝送信号に施すスクランブルの規則を定める鍵情報と、前記鍵情報に対して固有に割り当てられる鍵識別子と、特定受信局装置を示す宛先符号とを含んだデスクランブル許可情報を構成し、前記デスクランブル許可情報を前記伝送信号に多重して送出することにより、前記上記宛先符号で示された受信局装置が前記伝送信号のデスクランブルを実行できるようにしたスクランブル制御方法において、前記宛先符号と、前記鍵識別子と、前記鍵識別子で示される鍵情報の無効を示す情報とを含んだ鍵制御情報を構成し、前記鍵制御情報を特定の受信局装置宛に送出することによって、前記受信局装置に保管されている前記鍵識別子で指定された鍵情報を削除することを特徴とするスクランブル制御方法

(2) 鍵情報に応じた規則で伝送信号にスクラ

ンブルを施すスクランブル実行手段と、前記鍵情報と鍵識別子と宛先符号とを含んだデスクランブル許可情報を作成するデスクランブル許可情報作成手段と、前記鍵識別子と前記鍵識別子で示される鍵情報の無効を示す情報とを含んだ鍵制御情報を作成する鍵制御情報作成手段とを備え、前記デスクランブル許可情報と、前記鍵制御情報と、前記スクランブル実行手段で使用中の鍵情報に対応した鍵識別子とを、スクランブルされた伝送信号に多重して送出することを特徴とするスクランブル送信装置。

(3) 鍵情報と鍵識別子と宛先符号とを含んだデスクランブル許可情報を入力とし、前記宛先符号を照合して前記受信局装置宛のデスクランブル許可情報か否かを判断する宛先照合手段と、前記受信局装置宛のデスクランブル許可情報の鍵情報と前記鍵識別子を格納する鍵格納手段とを備え、スクランブルされた伝送信号を前記鍵情報に応じた規則でデスクランブルするとともに、前記鍵識別子と前記鍵識別子で示される鍵情報の無効を示

す情報とを含んだ鍵制御情報を入力とし、前記鍵識別子で示される鍵情報が前記鍵格納手段によって格納されているか否かを照合する鍵情報照合手段を備え、格納されていれば該当する鍵識別子と鍵情報を消去することを特徴としたデスクランブル受信装置。

3. 発明の詳細な説明

産業上の利用分野

本発明は、通信システムの分野に関連し、特に映像、音声等のデータ通信に使用するスクランブル制御方法に関する。

従来の技術

近年、通信衛星が打ち上げられ、テレビジョン信号等が衛星を利用して配信されるようになってきた。本社から全国各地の支店へ経営状況などを送る社内ネットワークが構築されているが、企業情報が他社に洩れないように内容の秘匿性が問題となっている。こうした要求を可能とするため、送信局でテレビジョン信号にスクランブルをかけて送出し、受信局ではデスクランブル受信装置を

設置して、デスクランブルして視聴する方法がとられるようになってきた。デスクランブルできる受信装置は、事前にデスクランブル許可を受けている特定の受信装置のみである。

従来のスクランブル制御方法において、特定の受信装置のみをデスクランブル可能とする制御方法は、郵政省昭和63年度電気通信技術審議会答申諮問第17号「放送衛星によるテレビジョン放送における有料方式に関する技術的条件」に示すような構成が一般的であった。以下、その構成について第4図、第5図、第6図を参照しながら説明する。

第5図において、送信局ではテレビジョン信号などの伝送信号11に施すスクランブルの規則を定める鍵情報6を、各鍵情報に固有な鍵識別子7と対にして鍵情報管理手段5で管理している。さらに、デスクランブルを許可する全ての受信装置の装置識別子1を受信装置管理手段2で管理している。

デスクランブル許可情報作成手段3では、第4

図に示すように、特定の受信装置の装置識別子1を宛先符号9とし、鍵情報6と鍵識別子7と鍵有効期限8と宛先符号9とを含むデスクランブル許可情報10を作成する。デスクランブルを許可する受信装置が複数台ある場合には、宛先符号ごとに1つのデスクランブル許可情報10を作成する。そして、スクランブル処理に先だって、事前にこのデスクランブル許可情報を多重手段4を介して送出する。

次に、テレビジョン信号などの伝送信号11を送出する際に、鍵情報6に定められた規則に従ってスクランブル実行手段12でスクランブルを施すと共に、使用した鍵情報6と対になっている鍵識別子7が何であるかを、多重手段4によってスクランブルされた伝送信号に多重して全受信装置に送る。

一方第6図において、受信装置には各受信装置ごとに固有の装置識別子1が割り当てられており、宛先照合手段20によって受信されたデスクランブル許可情報10中の宛先符号9と照合されるよ

うになっている。送信局から第4図に示す構成のデスクランブル許可情報10が送られてくると、宛先符号9が自身の装置識別子1と一致すれば、その中の鍵情報6と鍵識別子7の対を取り出して、鍵有効期限8に示された日時まで鍵格納バッファ21に格納しておく。

次に、スクランブルされた伝送信号13の受信時には、伝送信号と並行して送信局から送られてくる鍵識別子7が鍵情報検索手段22に入力され、鍵識別子7と同一の鍵識別子7'（数字の上のダッシュは鍵格納バッファに格納中の情報であることを示すものとする）が鍵格納バッファ21にあるか検索され、あれば鍵識別子7'と対になっている鍵情報6'がデスクランブル実行手段23に入力される。デスクランブル実行手段23では、鍵情報6'を用いて、スクランブルされた伝送信号13をデスクランブルし、デスクランブルした伝送信号24を出力する。したがって該当する鍵識別子7'と鍵情報6'を持たない受信装置はデスクランブルすることができない。鍵情報6'を

保有している受信装置であっても、鍵有効期限8'が経過した時点で鍵情報6'と鍵識別子7'を削除し、それ以降はデスクランブルできなくなる。

発明が解決しようとする課題

しかしながら従来の技術では、デスクランブル受信装置に格納された鍵情報を送信局からの指示によって強制的に削除する手段がなかったために、一度デスクランブル許可情報を受信し、鍵識別子と鍵情報を手に入れた受信装置は、その鍵情報を使用してスクランブルを施した伝送信号であれば、鍵有効期限の間は必ずデスクランブルが可能であった。

テレビジョン信号の場合は、送信局がテレビジョン信号の送出に先だって、各受信局を視聴可能にすべきかどうかを判断し、視聴可能とする受信局だけにデスクランブル許可情報を送信するが、一度視聴可能と判断してデスクランブル許可情報を送った受信装置を視聴不可能に変更することはできなかった。そのため、視聴可能から視聴不可能への変更は、デスクランブル許可情報を送る前に

ランブルが不可能な状態に変更できる。

実施例

以下、本発明の一実施例について第1図、第2図、第3図および第4図を参照しながら説明する。

第1図は、本発明によるスクランブル送信装置内部の構成を示すブロック図である。

同図に示すように、送信装置には、伝送信号11に施すスクランブルの規則を定める鍵情報6と名鍵情報6に対して固有に割り当てられる鍵識別子7の対を管理する鍵情報管理手段5と、その鍵情報6を使用してスクランブルを施した伝送信号のデスクランブルを許可する受信装置の装置識別子1を管理する受信装置管理手段2がある。受信装置管理手段2が管理している受信装置の装置識別子1を宛先符号9とし、第4図に示すように、この宛先符号9と鍵情報6と鍵識別子7と鍵有効期限8を含むデスクランブル許可情報10を許可情報作成手段3において作成する。そして、スクランブル処理に先だって、事前にこのデスクランブル許可情報10を、多重手段4を介して受信装置

決定しなければならないという制約があった。

本発明は上記課題を解決するもので、デスクランブル許可情報を送付した後に、視聴可能から視聴不可能への変更を可能とすることを目的としている。

課題を解決するための手段

本発明は上記目的を達成するために、宛先符号9と、鍵識別子7と、その鍵識別子で示される鍵情報の無効を示す情報とを含んだ鍵制御情報を構成し、送信局からこの鍵制御情報を送付し、宛先符号9で指定されるデスクランブル受信装置内に鍵識別子7が一致する鍵情報があれば、その鍵情報を削除することによって、受信側がデスクランブルできないようにするものである。

作用

本発明は上記した制御方法により、一度はデスクランブル許可情報を受信して鍵情報を手にいれた受信装置から、送信局の指示によって鍵情報を削除する手段を設けたことにより、一度許可を与えたスクランブル受信装置に対しても随時デスク

に送る。

次に、宛先符号9を指定してデスクランブル許可情報10を送った受信装置に対して、一度与えた許可を取り消してデスクランブルできないようにする必要が発生した場合、受信装置管理手段2によって管理されている装置識別子1と、鍵情報管理手段5によって管理されている鍵識別子7が鍵制御情報作成手段14に入力され、第3図に示すように、装置識別子1を宛先符号9とし、鍵識別子7とその鍵識別子で示される鍵情報の無効を示す情報15とを含んだ鍵制御情報16を作成する。鍵制御情報16は、多重手段4を介してデスクランブル許可を取り消すべき受信装置に送付される。

次に、テレビジョン信号などの伝送信号11を送出する際には、鍵情報管理手段5からスクランブル実行手段12に鍵情報6が入力され、伝送信号11にスクランブル処理が施される。そしてスクランブル処理と並行して、使用した鍵情報6と対になっている鍵識別子7が何であるかを、多重

手段4によりスクランブルされた伝送信号に多重して全受信装置に送る。

第2図は、本発明によるデスクランブル受信装置内部の構成を示すブロック図である。

受信装置においては、宛先照合手段20によってデスクランブル許可情報10内の宛先符号9が自身の装置識別子1であるか否かを判定し、他の受信装置宛のデスクランブル許可情報であれば捨て、自身宛のデスクランブル許可情報であれば鍵情報6と鍵識別子7の対が、鍵格納バッファ21で鍵有効期限8に示される日時まで保持される。

次に、送信局から鍵制御情報16が送られてくると、宛先照合手段20によって鍵制御情報16内の宛先符号9が自身の装置識別子1であるか否かを判定し、他の受信装置宛の鍵制御情報であれば捨て、自身宛の鍵制御情報であれば鍵情報照合手段25へ入力する。鍵情報照合手段25では、鍵制御情報16で送られてきた鍵識別子7と同じ鍵識別子が鍵格納バッファ21の中にあるかを調べ、あれば鍵情報削除手段26によって、鍵格納

バッファ21から該当する鍵識別子7と鍵情報6の対を削除する。

次に、スクランブルされた伝送信号13の受信時には、伝送信号と並行して送信局から送られてくる鍵識別子7が鍵情報検索手段22に入力され、鍵識別子7と同一の鍵識別子7'が鍵格納バッファ21にあるか検索され、あれば鍵識別子7'と対になっている鍵情報6'がデスクランブル実行手段23に入力される。デスクランブル実行手段23では、鍵情報6'を用いて、スクランブルされた伝送信号13をデスクランブルする。このとき、デスクランブル許可情報10が送られてこなかった受信装置、あるいはデスクランブル許可情報10が送られてきた後に鍵制御情報16が送られてきて鍵識別子7と鍵情報6を削除した受信装置は、鍵情報検索手段22による検索で該当する鍵識別子を見つけられないので、デスクランブルを実行することができない。鍵情報6'を保有している受信装置では、鍵有効期限8'が経過した時点で鍵情報6'と鍵識別子7'を削除し、それ

以降はデスクランブルできなくなる。

このように本発明の実施例のスクランブル制御方法とその方法に従った装置によれば、デスクランブル許可情報10によって受信装置に一度与えた鍵情報6'を、送信局からの鍵制御情報16によって削除する手段を設けたことにより、デスクランブル許可情報10を送った後にも再度、デスクランブル不可能に変更できる。

なお、上記の説明における送信装置と受信装置の構成はハードウェアによるブロック図で示したが、その処理をマイクロプロセッサ等によるソフトウェア処理で容易に実現することもできる。

また、デスクランブル許可情報と鍵制御情報を受信装置へ送出する方法については、伝送信号と多重して送出するかわりに、ICカードのようなパッケージメディアによる受渡しでおきかえることも可能である。

発明の効果

以上のように本発明によれば、送信局からの制御信号によって受信装置内の鍵情報を強制的に削除

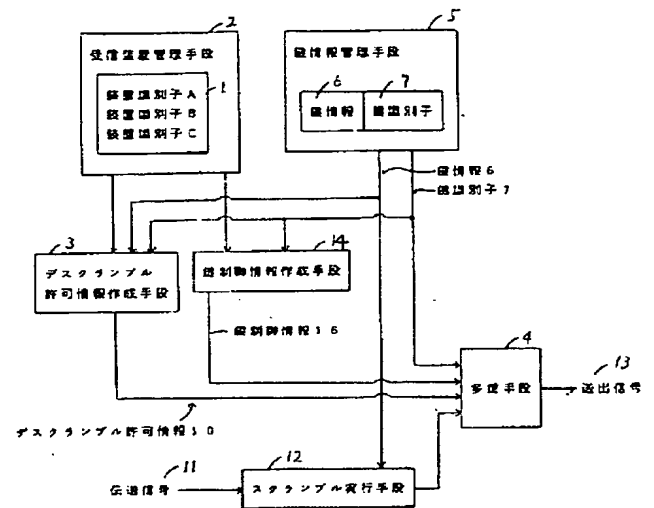
する手段を設けたために、一度伝送信号のデスクランブルを可能とした受信装置をデスクランブル不可能に変更することができるようになり、デスクランブル許可情報の送出の前後に関係なくデスクランブルの可能不可能を変更できる。テレビジョン信号の場合には、デスクランブル許可情報を送った後でも、視聴可能から視聴不可能への変更を決定できるようになり、使い勝手のよいスクランブル装置を提供できる。

4. 図面の簡単な説明

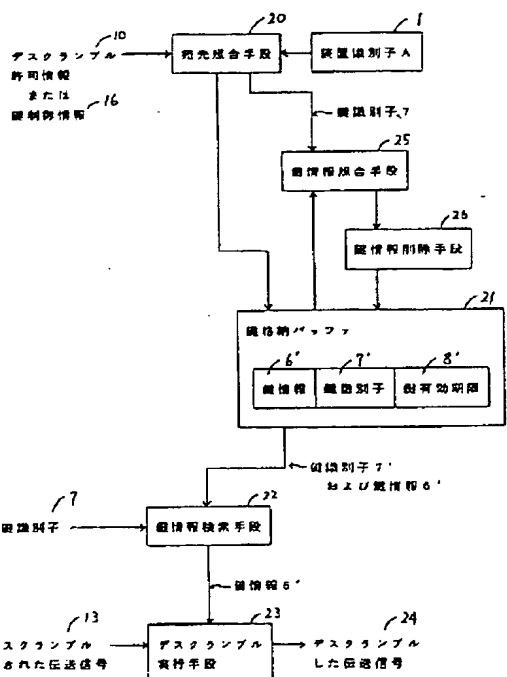
第1図は本発明の一実施例のスクランブル送信装置の内部構成を示すブロック図、第2図は同デスクランブル受信装置の内部構成を示すブロック図、第3図は鍵制御情報の構成を示す図、第4図はデスクランブル許可情報の構成を示す図、第5図は従来のスクランブル送信装置の内部構成を示すブロック図、第6図は同デスクランブル受信装置の内部構成を示すブロック図である。

1.....装置識別子 2.....受信装置管理手段
3.....デスクランブル許可情報作成手段 6.....

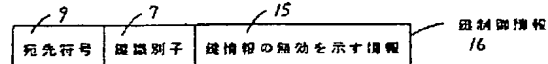
鍵情報 7鍵識別子 9宛先符号
 10デスクランブル許可情報 11伝
 送信号 12スクランブル実行手段 14
鍵制御情報作成手段 15鍵情報の無効
 を示す情報 16鍵制御情報 20宛
 先照合手段 25鍵情報照合手段
 代理人の氏名 弁理士 小 坂 治 明 ほ か 2 名



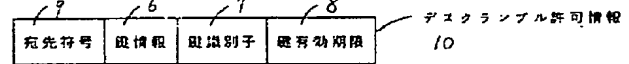
系1図



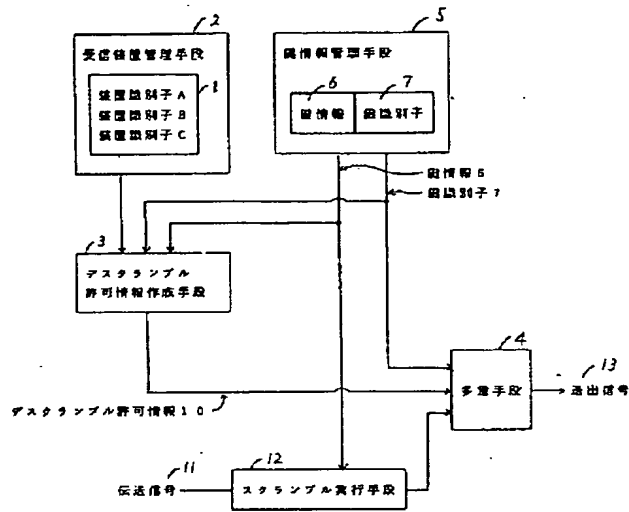
第2図



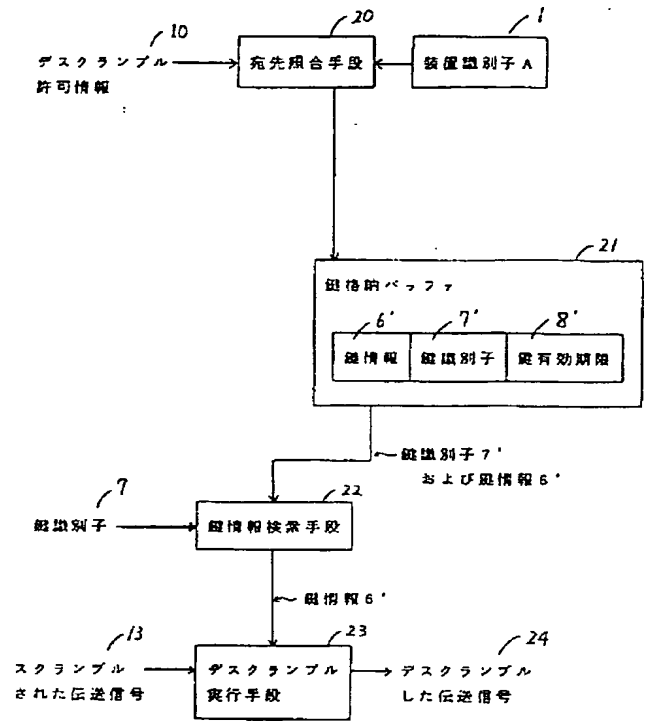
第3図



第4図



第5図



第6図